Institute for Pure and Applied Mathematics, UCLA, California
29 August 2012

Technology and Novel Protocols for Quantum Noise Protected Communication

Prem Kumar
Center for Photonic Communication and Computing
Northwestern University
kumarp@northwestern.edu

Gregory S. Kanter
NuCrypt, LLC
1840 Oak Ave. Suite 212-S, Evanston, IL 60201-3697
kanterg@nucrypt.net

Overview

- Physical Security vs. Traditional Cryptography
- AlphaEta: Quantum Noise Enhanced Encryption
- OCDMA Using Dynamic (Running) Codes
- QKD Security
- Keyed QKD Protocols
- Tools for Quantum Communications:
  - Single Photon Detectors
  - Entanglement Sources

Why Physical Cryptography (Security)?

1. Different (most important?)

- like redundant systems, want security 'layers' to be as independent as possible
- potential new physical burdens on the attacker, e.g., wide-band coherent measurement
- technology developments can be harder to hide than algorithmic developments
- ***logistical burden*** (measurement tools at right place at the time message sent)

2. New tools to enhance standard cryptography

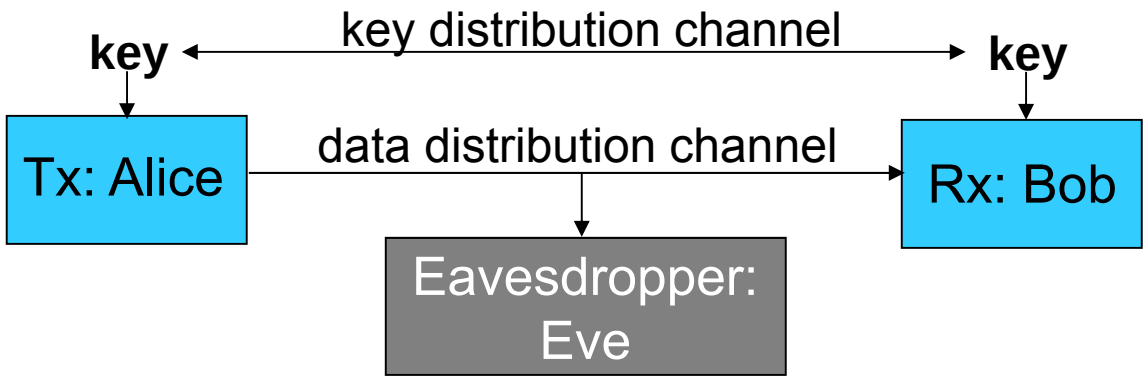
digital processor	→	physical processor (chaotic lasers)
'mixing': S-boxes and permutations	→	mixing: high speed RNG (quantum noise)
Assumed difference in Bob vs. Eve signal quality	→	Guaranteed difference (quantum effect)

3. Some methods have potential for provable 'information theoretic' security

Traditional cryptography is great but 'proofs' tied to strong computational assumptions

- how hard is it to compute an inverse log or to factorize a composite number?

Cryptography

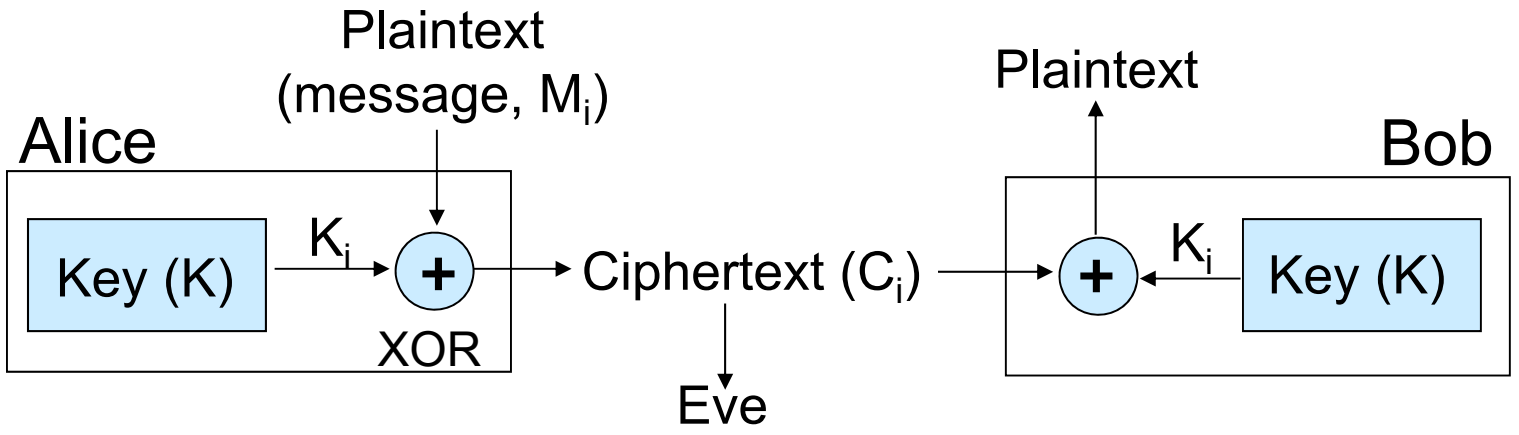


Encryption:
- Protects message from unauthorized observation
- Knowledge of a key (or some secret) identifies legitimate users
- Typically key is short (<1000 bits) while the message is long (>Gb)

Key Distribution:
- Generate shared key between two users
- Some initial shared secret generally needed for authentication
- Traditionally use 'one-way' mathematical functions

Authentication (verify sender and integrity), Non-Repudiation, etc.

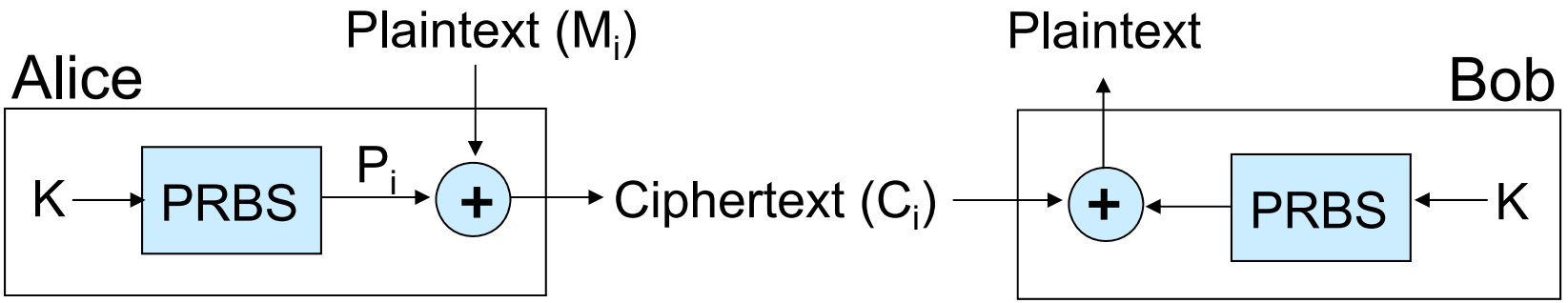
One Time Pad Encryption
(Vernam Cipher)



- **Only *Perfect* encryption**
  - Ciphertext is statistically independent of message
- **Key needs to be truly random and only used once**
- **Why is it so special?**
  - Eve has ***exactly*** guessing probability on each bit and ***no*** correlations between bits
  - Simple protocol ($C_i = M_i \oplus K_i$)

    No Hash, Error Correction, Privacy amplification, Pseudo-Random Number Generation
  - *Not just because it is "information theoretically" secure**!***
- **Key length = message length (impractical)**

Efficient Encryption



Pseudo-Random Bit Sequence (PRBS)

- Convert short key K to long output P_i and treat it as if a One Time Pad (it is not though!)
- Want computationally infeasible to find K from P_i (How to prove this?)

Advanced Encryption Standard (AES)

no practical attacks known

(some weaknesses identified)

Linear Feedback Shift Register (LFSR)

can convert P to K if: i ~ key length

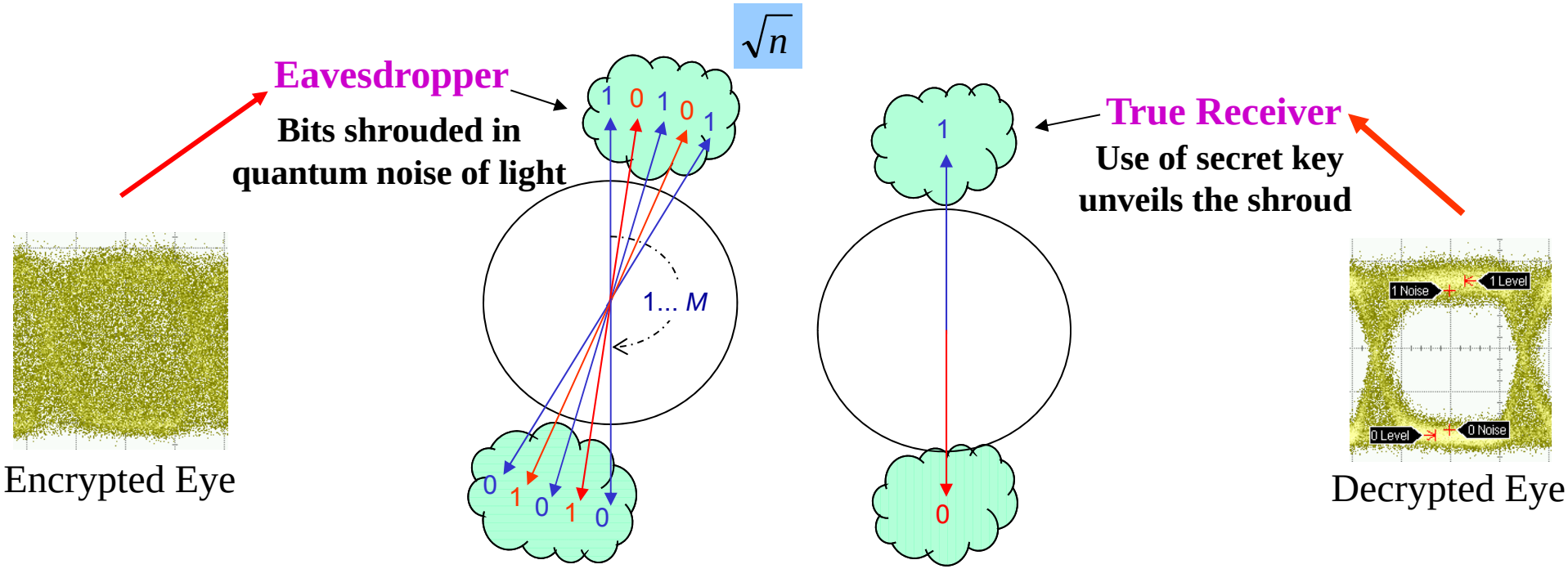
(a few words for a 128 bit key)

What if we assume M_i is random (cipher-text only attack)?

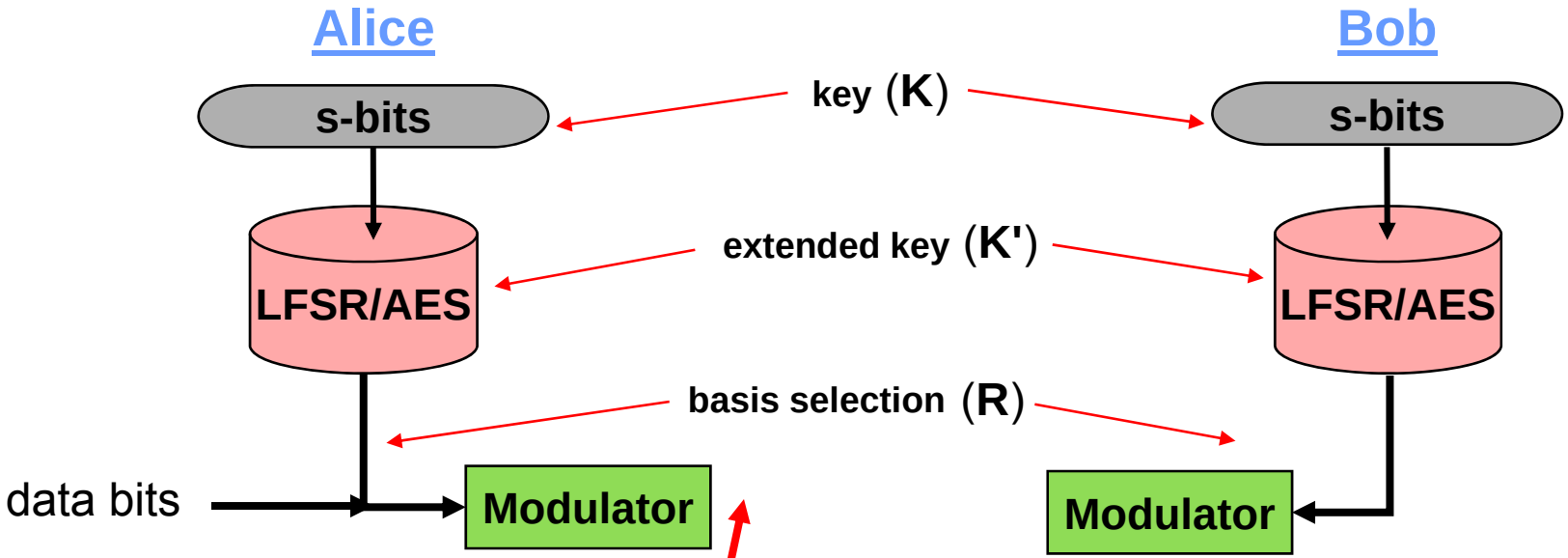
- M_i is like a one-time pad: P_i and thus key is perfectly secure (for all algorithms)
- This is really meaningless (composability problem)

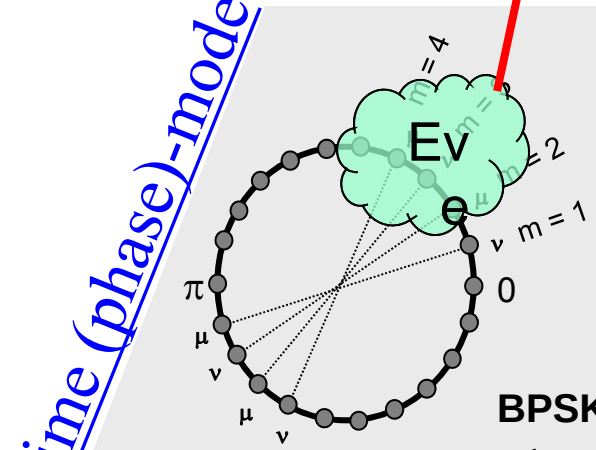
AlphaEta: Quantum-Noise Enhanced Data Encryption

- Ciphers strive to look “random” but are deterministic algorithms
- Eve sees an analog-like signal (sensitive to noise), actual users see digital
- *Unavoidable* quantum noise randomizes the observed output of cipher
- Ultra-secure encryption for medium rate optical communications
  - drawback: *rate is limited by DAC technology*
- Maintain performance and compatibility with typical WDM systems
- Use commercially available off-the-shelf components



AlphaEta Protocol
Quantum Data Encryption (QDE)





M bases (2M phase states), *m*:[0,M-1]

$$\left|\psi_m^{(\mu)}\right\rangle = \left|\alpha e^{i\theta_m}\right\rangle$$

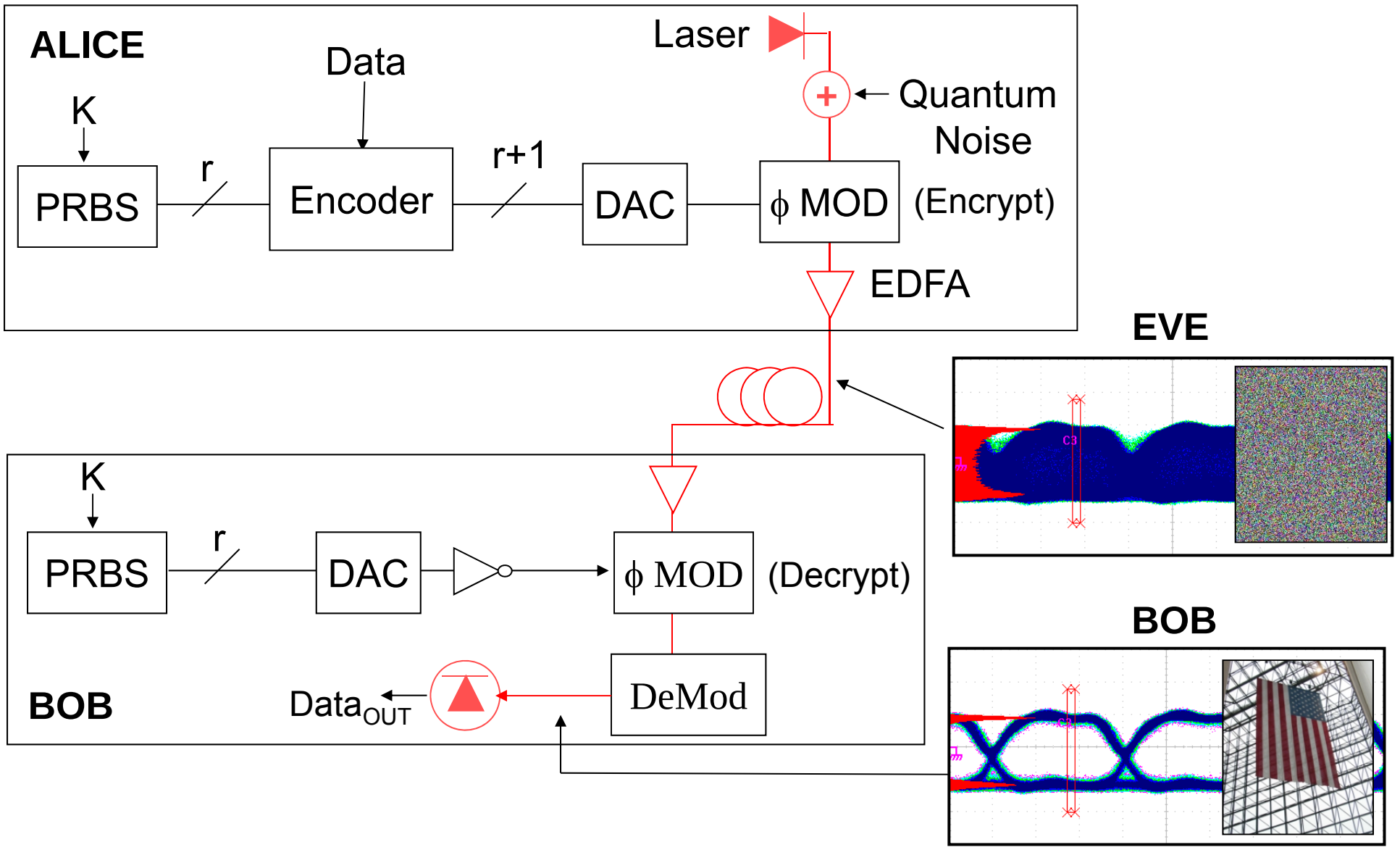
$$\left|\psi_m^{(\nu)}\right\rangle = \left|\alpha e^{i(\theta_m+\pi)}\right\rangle$$

BPSK logical encoding:

$$\{\mu\mu,\nu\nu\} \rightarrow L1 \quad \{\mu\nu,\nu\mu\} \rightarrow L0$$

Corndorf *et al*., Optics Letters **28**, 2040 (2003); Phys. Rev. A. **71**, 062326, (2005)

AlphaEta Block Implementation



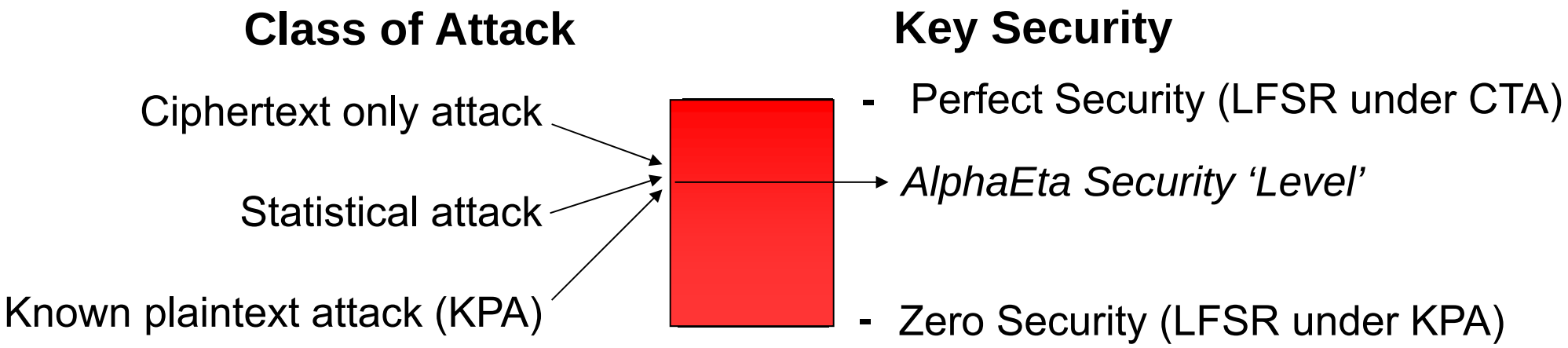
AlphaEta Security

- 'Lower bound' noise levels for Eve's statistical analysis known precisely
- Security 'Level' depends on:

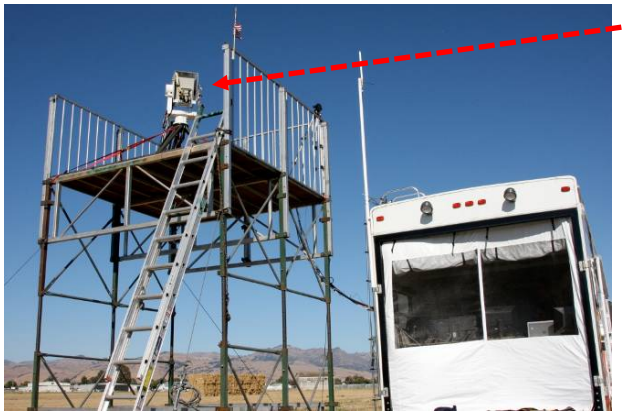
  amount of noise, type of PRBS algorithm used (LFSR or AES), # basis states
- Still may not know exactly how hard system is to break

  (if optimal breaking algorithm unknown - e.g., AES) but:

  - *worst-case security improved (even simple LFSR can offer useful security)*
  - *quantum noise randomization adds qualitatively different type of security*
  - *nebulous problem of Eve's statistical knowledge circumvented*



Notable AlphaEta Experiments

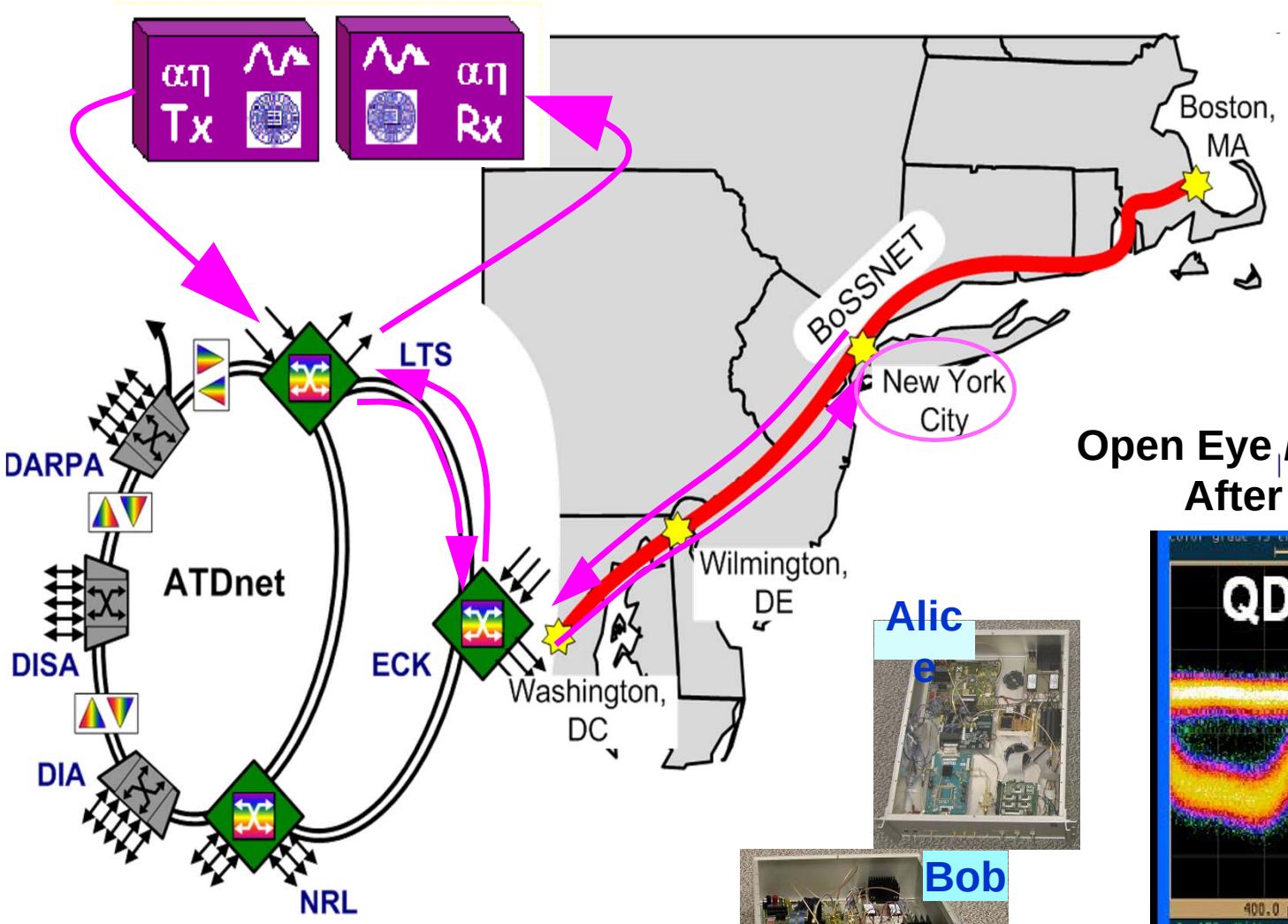


- **>500km at 2.5Gb/s (256 states), DPSK[1]**
- **>300km at 10Gb/s (64 states), ASK[2]**
- **~850km at 622Mb/s over ATDNet / BOSNET installed fiber network[3]**
- **20km at 2.5Gb/s mobile airplane-to-ground free space link[4]**

1. G. S. Kanter *et al.*, IEEE Communications Magazine, 2009.
2. Y. Doi *et al.*, OFC 2010.
3. T. Banwell *et al.*, Milcom 2005
4. AOptix / NuCrypt press release, 2009

Telcordia / Northwestern University ATDNet / BOSSNET OC-12 Demonstration

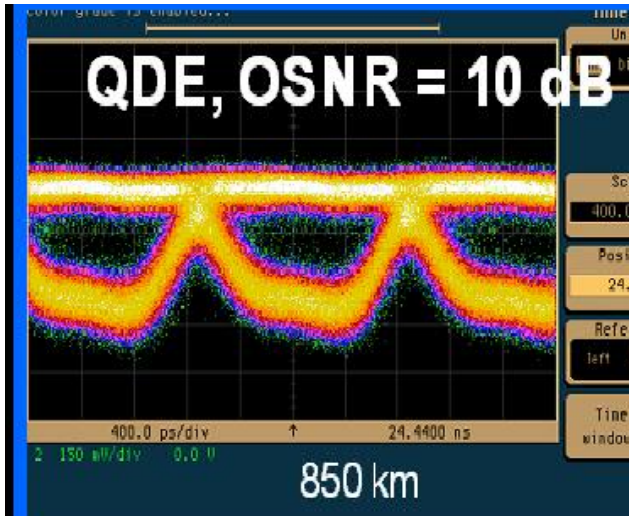
850km loop: Maryland to New York and back



System setup

- 850 km round-trip transmission path
- Mixed networks (ATDnet & BoSSNET) & fiber types

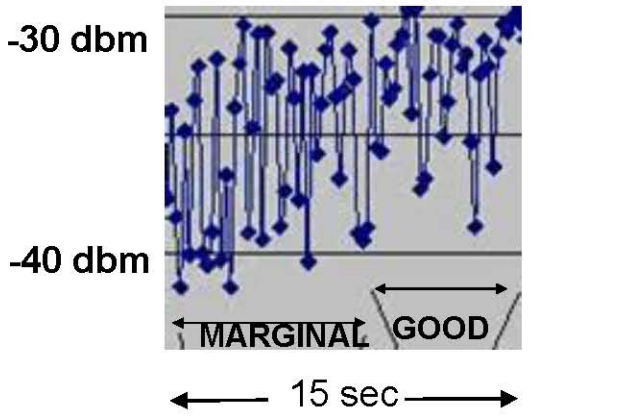
Open Eye / FEC Correctable BER After 850km (622Mb/s)



T. Banwell *et al.*, MilCom 2005

Alpha-Eta Coherent "State Quantum Data Encryption" (QDE) Stationary Experiment

Snapshot Minimum Received Power



Average Received Power: - 22 dbm

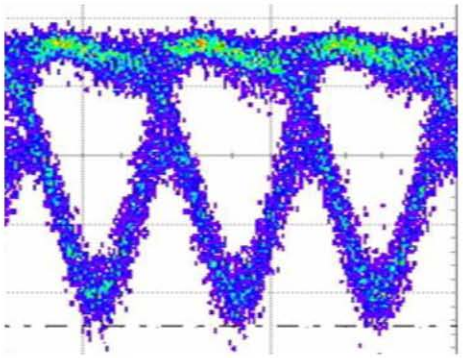
Objective: Determine feasibility of NuCrypt LLC's phase based Alpha-Eta QDE stationary transmission through a turbulent atmosphere

Approach: Utilize AOptix "curvature" adaptive optics terminals to compensate for **wave-front phase distortions** over a ten kilometer link

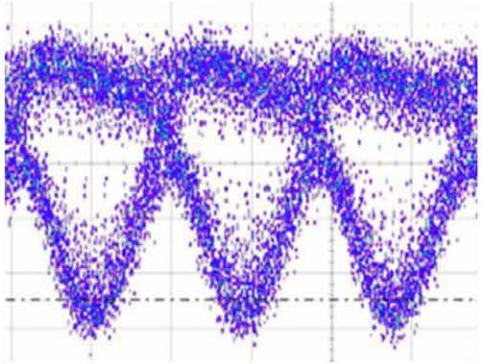
Result: Successful demonstration of QDE transmission, and decryption inversion over 10 km free space link.

Eye Diagrams Illustrating successful decryption of random bit stream

Control (Inside) Simulated Turbulence

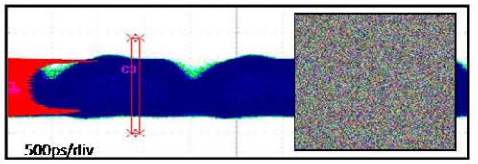


Actual (Outside) Real Turbulence

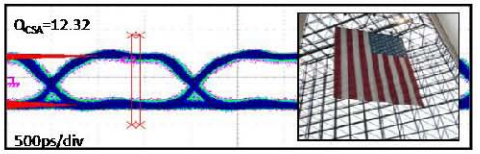


Example:

Encrypted Image

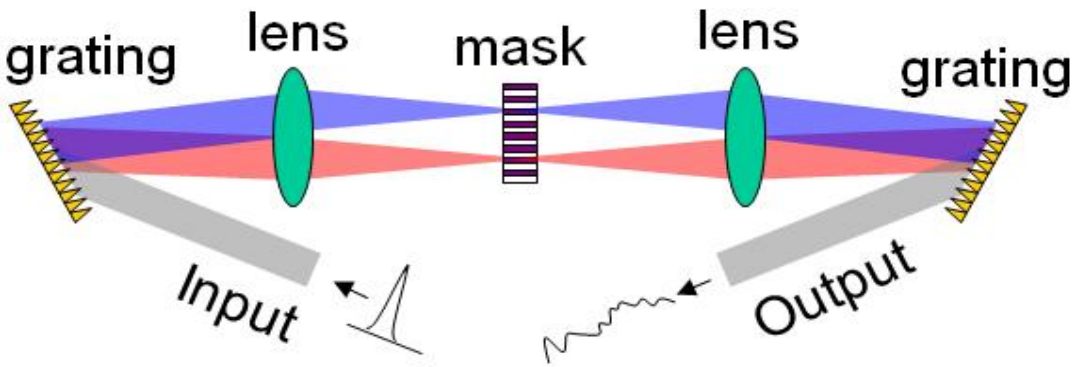


Decrypted Image



SPE-Based OCDMA

Spectral Phase Encoding (SPE)



$$E_{out}(\omega) = E_{in}(\omega)\underbrace{H_M(\omega)}$$

Mask Spectral Function

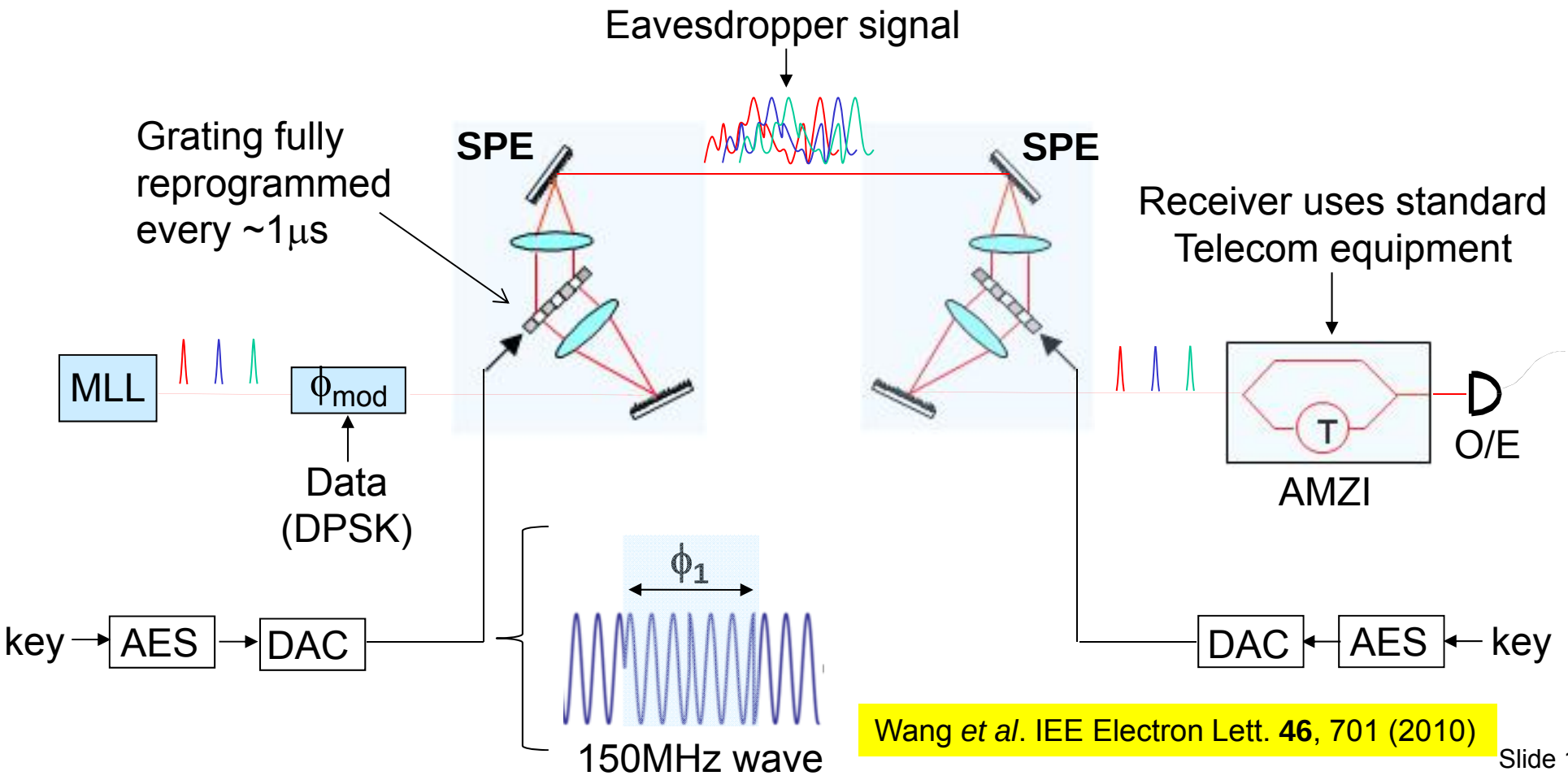
- Break pulse up into multiple spectral components
- Apply phase shift to each frequency bin
- Can multiplex channels based on spectral code (like CDMA)
- Receiver needs opposite mask to re-compress pulses

  - also means to handle interference (fast time-gate or balanced DPSK)
- Wide optical bandwidths (harder to measure)

  - say 200GHz optical BW, so >400Gs/s, or ~2Tb/s of data
- ***No electronics*** and works at high rates but susceptible to mask attacks

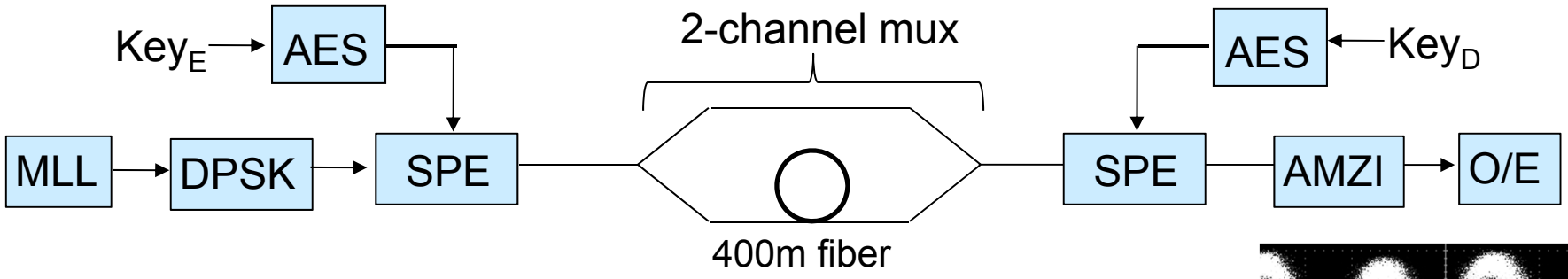
Running-Code OCDMA

- **Use acousto-optical modulator (AOM) pulse-shaper**
- **RF-phase controls spectral phase shift**
- **Dynamically change RF phase with DAC (phase shift fed from AES) (50ns partial change, 2μs full refresh)**



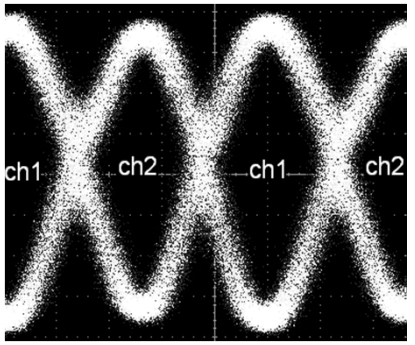
Wang *et al*. IEE Electron Lett. **46**, 701 (2010)

Running-Code OCDMA Experiment

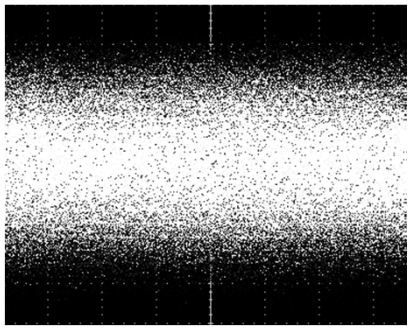


- **Emulate 2x10Gb/s system**
- **~25 spectral bins with 128 phase levels/bin**
- **Pulses spread several bit slots**
- **~190GHz FWHM optical bandwidth**
- **Recover channel with synched decryption**

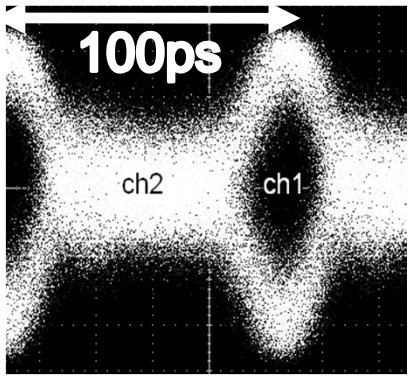
No SPE



Key$_E$≠Key$_D$



Key$_E$=Key$_D$,
Ch1 sync



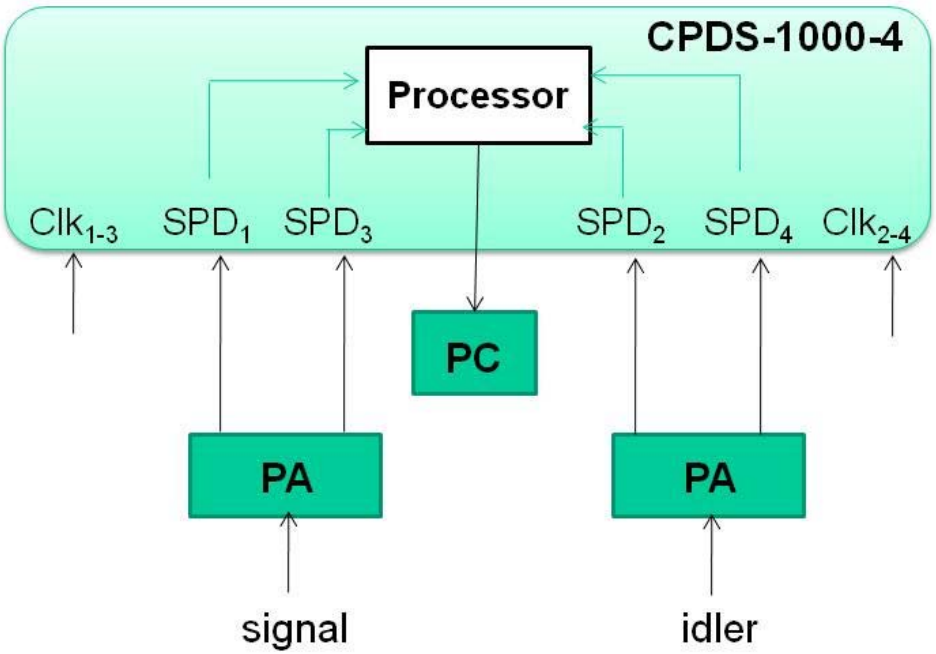
Ozharar *et al*. J. Lightwave Technol. **29**, 2081 (2011)

Single Photon Detection

- Commercial detectors have high efficiency (>25%) and low afterpulsing (<1%) but slow
- Research results faster, but often detection efficiency low (10%) or afterpulsing high (5%)
- At high rates required processing such as afterpulse masking are harder to implement
- Best performing research systems are inflexible - e.g., small rate range
- No commercially available high rate detectors yet - much less systems

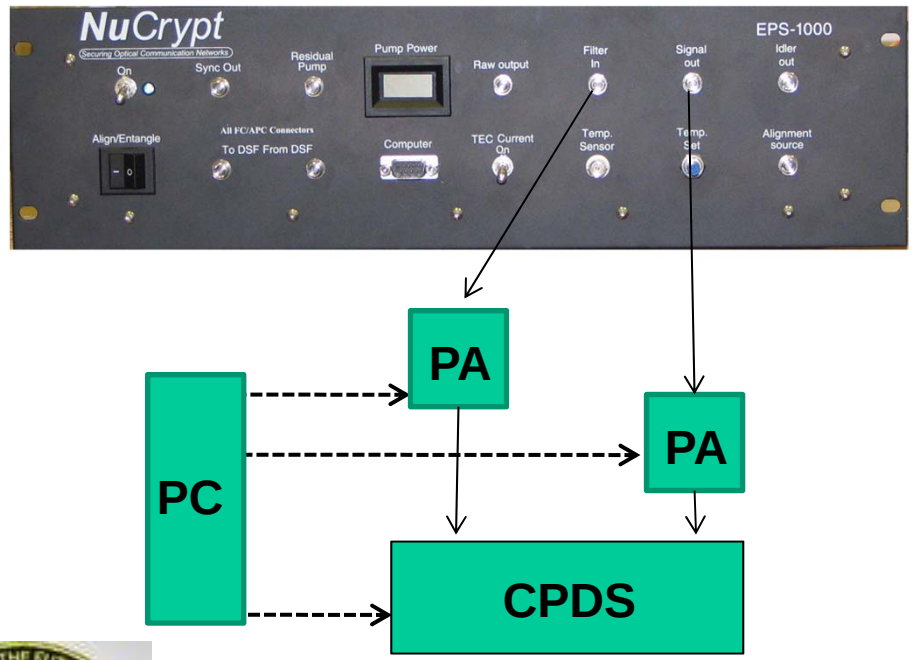
NuCrypt System

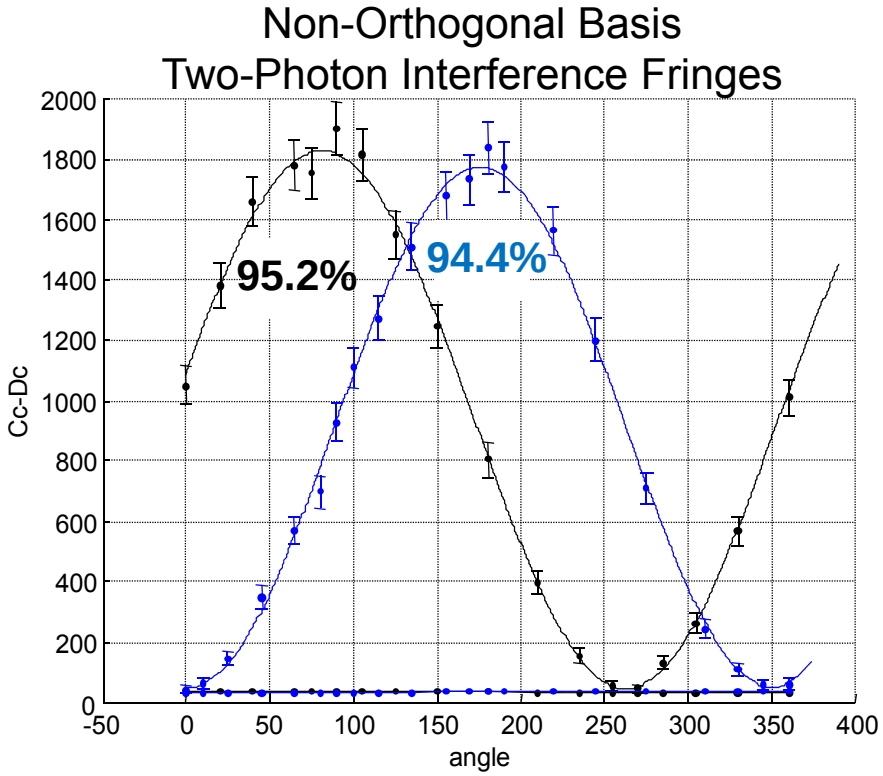
- 50MHz - ***faster*** systems in development
- Up to 4 detectors with statistics recorded
- Compatible with electronically controlled Polarization Analyzer (PA)
- ~2% afterpulsing before masking
- >20% efficiency
- Available for purchase



Entangled Photon Source (EPS)

- Internally generated alignment signals
  - easily compensate for fiber birefringence between EPS and PA
- {98,95,92}% Two Photon Fringes with fiber at {-196, -80,+25}°C
- 3 entangled pairs at different wavelengths can be generated by one EPS
  - central EPS can distribute entanglement to multiple pairs of users



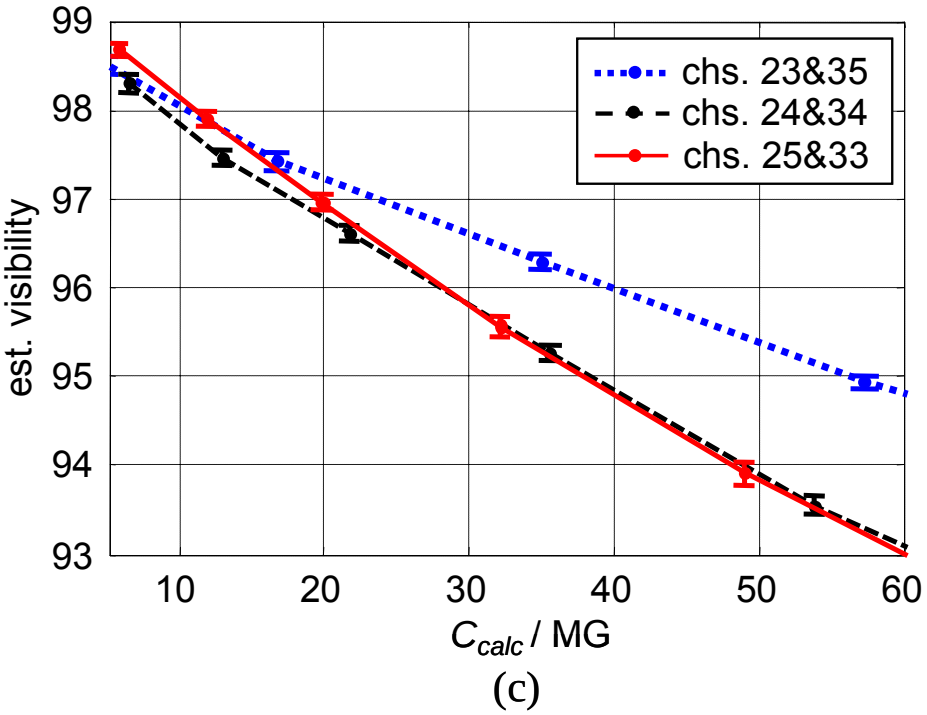


PA: Polarization Analyzer
CPDS: Correlated Photon Detection System

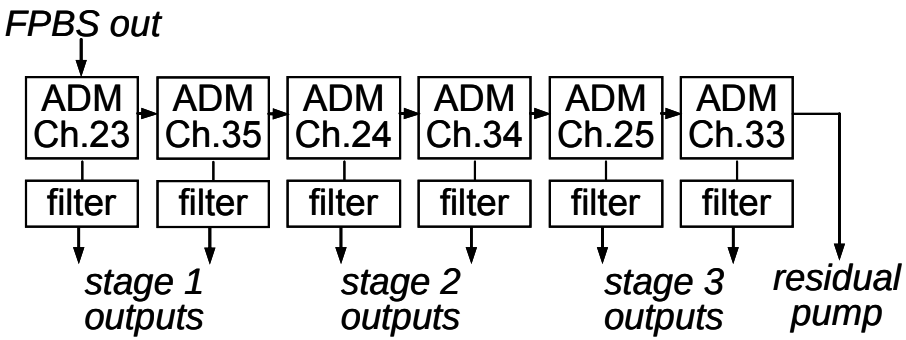
Practical Performance Issues

- Performance (two photon interference visibility and rate) depends on:

  -detector characteristics, fiber loss, two-photon generation rate, Raman photons
- Fast method of setting basis and tracking fiber birefringence (if polarization entangled)
- Multiple simultaneous users from single EPS- frequency entanglement issue?
- Wavelength: 1310nm- low interference, 1550nm- low fiber loss, <900nm- Si detectors

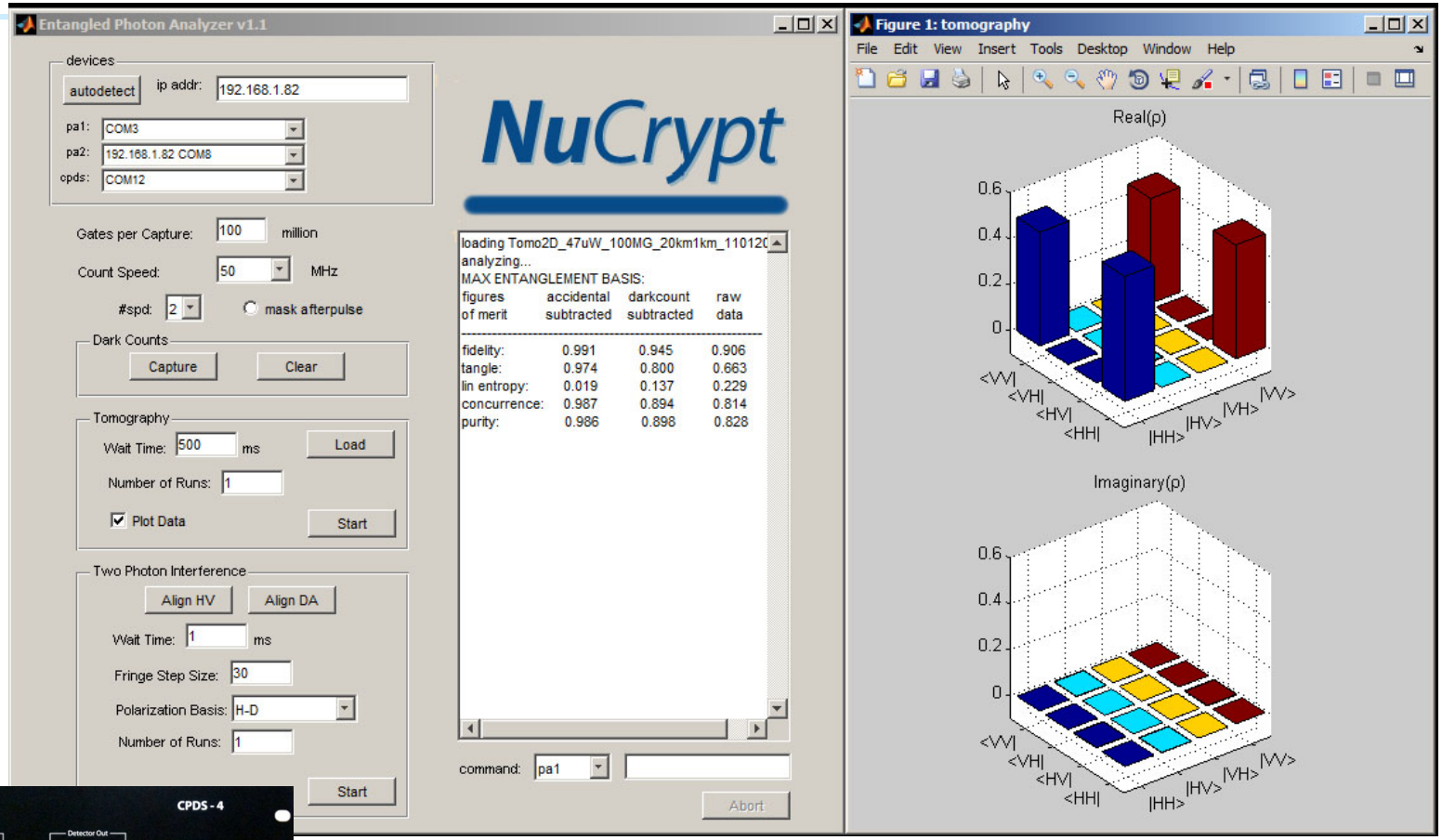


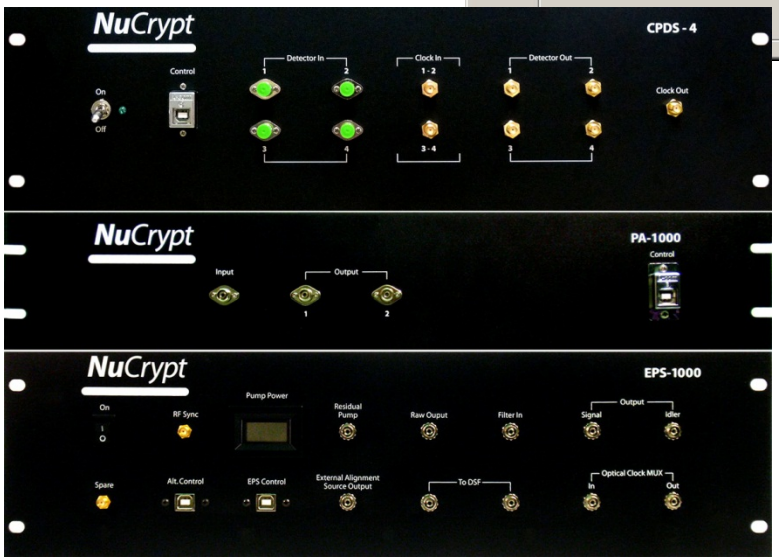
(c)



(a)

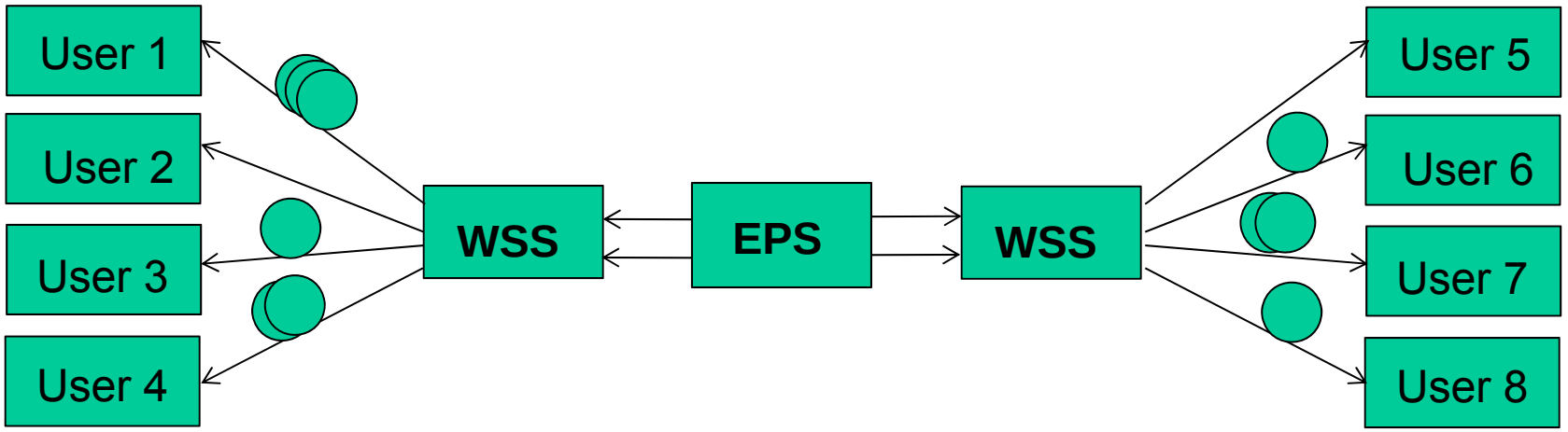
Quantum State Tomography System





Potential Future Directions

- Entanglement distribution through turbulence (quantum networks)
- Entanglement (QKD) distributed efficiently in fiber networks: central EPS
- Commercialize entanglement systems for plug-in generation and measurement
  - entanglement type: polarization, time-bin, hyper-entangled, and degenerate
  - include important 1310nm wavelength, possibly others
  - room temperature operation using holey fiber
- Keyed QKD systems with high practical security
- Mid-rate (2.5-10Gb/s) AlphaEta quantum noise enhanced cryptosystems
- Physically secure high-rate OCDMA networks: say 4x100Gb/s



Summary

- Physical effects bring new tools for securing communications
- Technology burdens can be important
  - orthogonal to traditional cryptographic security assumptions
  - logistical and economic burdens
- Quantum noise can be used to enhance the security of standard ciphers
  - compatible with existing high-rate WDM systems
  - simple hacking attempts were unsuccessful, but more work is needed
- Standard ciphers can be used to enhance the security of OCDMA
- Truly provable security is difficult to achieve
  - quantum effects *should* lead to (qualified) provable security models, but fragile
- Quantum systems generally need quantum tools:
  - develop fast correlated single photon detection systems
  - develop user friendly entangled photon sources